THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI

REBECCA BLOUNT and CHERYL MCCULLEY, on behalf of themselves and all others similarly situated, Plaintiffs, -against- CERNER CORPORATION D/B/A ORACLE HEALTH, Defendant.	Case No. 4:25-cv-00259-BP **FIRST AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Rebecca Blunt and Cheryl McCulley, individually and on behalf of all similarly situated persons, allege the following against Cerner Corporation d/b/a Oracle Health ("Oracle Health," "Oracle" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

INTRODUCTION

1. Plaintiffs bring this class action against Cerner Corporation d/b/a Oracle Health[1] for its failure to properly secure and safeguard Plaintiffs' and Class Members' personally identifiable information ("PII") and protected health information ("PHI" and collectively with PII, "Private Information") from cybercriminals.

[1] Plaintiffs file this First Amended Class Action Complaint to correct a scrivener's error regarding the naming of a corporate defendant for which there are numerous "Oracle" entities.

2. Defendant Oracle Health is a healthcare software-as-a-service (SaaS) company offering electronic health record ("EHR") and business operations systems to hospitals and healthcare organizations.[2]

3. Oracle Corporation acquired the medical records giant Cerner Corporation for $28.3 billion in 2022,[3] making Oracle the second largest EHR vendor in the United States, providing EHR services to over 20 percent of the U.S. hospitals.

4. After being acquired by Oracle Corporation in 2022, Cerner was merged into Oracle Health, with most of its systems migrated to Oracle Cloud.[4]

5. In the course of doing business, Defendant is entrusted with the Private Information that patients provide to Defendant's customers.

6. Oracle Health's security failures led to cyberattack that compromised its legacy Cerner data migration servers that store patient data for multiple US healthcare organizations and hospitals.[5]

7. According to a notice sent to impacted Oracle Health customers, on or about February 20, 2025, Oracle Health learned that cybercriminals had gained access to patient information that was "on an old legacy Cerner server that was not yet migrated to the Oracle Cloud."[6]

---

[2] *See* https://www.oracle.com/health/

[3] *See* https://www.oracle.com/corporate/; https://www.cnbc.com/2025/03/06/oracles-federal-electronic-health-record-suffered-nation-wide-outage-.html (last visited Apr. 9, 2025).

[4] *See* Bleeping Computer, *Oracle Health breach compromises patient data at US hospitals* (March 28, 2025), https://www.bleepingcomputer.com/news/security/oracle-health-breach-compromises-patient-data-at-us-hospitals/

[5] *See id*.

8. Oracle Health revealed that a cybercriminal used compromised customer credentials to breach the server sometime after January 22, 2025, and copied data including patient Private Information, to a remote server (the "Data Breach").[7]

9. BleepingComputer, a website covering technology news, reported that the impacted hospitals are now being extorted by a threat actor named "Andrew," who is demanding millions of dollars in cryptocurrency not to leak or sell the stolen data and who has created websites about the Data Breach to pressure the hospitals into paying the ransom.[8]

10. This massive Data Breach has been revealed just a few days after it became known that another cybercriminal known as "rose87168" has accessed Oracle Cloud's "federated login infrastructure" and allegedly stolen approximately 6 million sensitive records potentially affecting more than 140,000 Oracle Cloud tenants worldwide.[9]

11. Oracle Health has been denying both breaches despite hackers offering proof of the sensitive data exfiltrated from Oracle Health's networks and/or servers, leaving millions of customers at risk.[10]

---

[6] *Id.*

[7] *See id.*
[8] *See id.*

[9] *See* USDM Life Sciences, *Oracle Breaches: What Happened and What's Next* (April 2, 2025), https://usdm.com/resources/blogs/oracle-health-breach-what-life-sciences-cybersecurity-leaders-need-to-know-and-do-now

[10] *See Oracle Health suffers major breach, hospital data potentially exposed* (March 31, 2025), https://www.techradar.com/pro/security/oracle-health-suffers-major-breach-hospital-data-potentially-exposed

12. Upon information and belief, the information compromised in the Cerner Data Breach included a variety of certain Private Information entrusted to and maintained by Oracle Health, including Private Information of Plaintiffs and Class Members.

13. Oracle Health's lack of transparency and proper notification, including its failure to provide official written reports to affected hospitals or to send data breach notices to affected patients and other victims,[11] is not only frustrating but puts Plaintiffs and Class Members at significant risk of identity theft and various other forms of personal, social, and financial harm. This substantial and imminent risk will remain for their respective lifetimes.

14. Oracle Health's denials of the Data Breach and its inadequate response to the cyberattack exacerbate the risk for the victims because 1) Oracle has not provided any notice of the Data Breach to Plaintiffs or Class Members; 2) Oracle has not informed Plaintiffs and Class Members whether it was able to fully contain or end the cybersecurity threat to their patient data, leaving victims to fear that their Private Information maintained by Oracle is not secure; and 3) Oracle has not disclosed the causes and the details of how the Data Breach occurred.

15. Armed with the Private Information accessed in the Data Breach, the cybercriminals who carried out the Data Breach can and will commit a variety of crimes, including, *e.g.*, obtaining medical services and/or prescriptions in Class Members' names, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining

[11] *See Oracle Health breach compromises patient data at US hospitals, supra* note 4.

driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

16. There has been no assurance offered by Oracle that all personal data or copies of data have been recovered or destroyed, or that it has adequately enhanced its data security practices to avoid a similar breach of its computer systems and networks in the future.

17. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

18. Plaintiffs bring this class action lawsuit to address Oracle's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

19. The Data Breach is a direct result of Oracle's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect individuals' Private Information with which it was entrusted.

20. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Oracle, and thus Oracle was on notice that failing to take necessary steps to secure the Private Information it left vulnerable to an attack.

21. Upon information and belief, Oracle failed to properly monitor and implement adequate data security practices with regard to its computer network and systems that contain Plaintiffs' and Class Members' Private Information. Had Oracle properly monitored its networks

and servers and implemented adequate data security practices, it could have prevented the Data Breach or, at the very least, discovered the Data Breach sooner.

22. Plaintiffs' and Class Members' identities are now at a current, imminent, and ongoing risk of fraud and identity theft because of Oracle's negligent conduct, which led to the Private Information that it collected and maintained falling into the hands of data thieves and other unauthorized third parties.

23. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that the Plaintiffs' and Class Members' Private Information was targeted, accessed, has been misused, and disseminated on the dark web.

24. Plaintiffs and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiffs and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts include and will continue to include in the future, among other things: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

25. Plaintiffs and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (g) deprivation of value of their Private Information; and (h) the continued risk to their sensitive Private Information, which remains in the possession of Defendant, and which is subject to further

breaches, so long as Oracle fails to undertake appropriate and adequate measures to protect it collected and maintained.

26. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and exfiltrated during the Data Breach.

27. Accordingly, Plaintiffs and Class Members bring this action against Oracle seeking redress for its unlawful conduct and asserting claims for: (i) negligence; (ii) breach of third-party beneficiary contract; (iii) breach of implied contract; (iv) unjust enrichment; (v) breach of confidence; (vi) breach of fiduciary duty; (vii) bailment; (viii) invasion of privacy; (ix) violations of the California Consumer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*; (x) violations of the California Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.*; (xi) violations of the California Unfair Competition Law, Cal. Bus. & Prof. Code §17200 *et seq.*; (xii) violations of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150.

PARTIES

28. Plaintiff Rebecca Blount is, and at all times mentioned herein was, an individual citizen of the State of Arizona residing in Pinal County, Arizona.

29. Plaintiff Cheryl McCulley is, and at all times mentioned herein was, an individual citizen of the State of California residing in Lassen County, California.

30. Defendant Cerner Corporation d/b/a Oracle Health is a Delaware corporation with its headquarters located at 8779 Hillcrest Road, Kansas City, Missouri 64138.

JURISDICTION AND VENUE

31. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of

interest and costs. Upon information and belief, the number of class members is over 100, many of whom including Plaintiffs have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

32. This Court has personal jurisdiction over Defendant because it operates in and has its principal place of business in this District, and conducts substantial business in this District.

33. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District, Defendant has its principal place of business in this District, and Defendant has harmed Class Members residing in this District.

FACTUAL ALLEGATIONS

A. Oracle's Business and Collection of Plaintiffs' and Class Members' Private Information

34. Oracle Health, formerly known as Cerner Corporation, is a US-based, multinational provider of various health information technology platforms and services, including EHR systems and software.

35. As a condition of receiving medical services from Oracle's customers in the healthcare industry, patients are required to entrust it with highly sensitive personal and health information.

36. On information and belief, in the ordinary course of their business of providing medical services, Oracle maintains the Private Information of consumers and their patients, including but not limited to:

a. Name, address, phone number and email address;

b. Date of birth;

c. Demographic information;

d. Social Security number;

e. Information relating to individual medical history;

f. Information concerning an individual's doctor, nurse or other medical providers;

g. Health insurance information;

h. Clinical testing information and results;

i. Other information that Defendant may deem necessary to provide services and care.

37. The information held by Defendant in its computer systems and servers included the unencrypted Private Information of Plaintiffs and Class Members.

38. Upon information and belief, Defendant made promises and representations to its patients that the Private Information collected from them as a condition of obtaining healthcare services from Defendant's customers would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.[12]

39. Thus, due to the highly sensitive and personal nature of the information Oracle acquires and stores with respect to its clients' patients, Oracle promises to, among other things, keep its clients' patients' Private Information private; comply with industry standards related to data security and the maintenance of patients' Private Information; inform patients of its legal duties relating to data security and comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to

[12] Indeed, one of Defendant's privacy policies provides that: "Oracle has implemented and will maintain technical and organizational measures designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Services Personal Information. These measures, which are generally aligned with the ISO/IEC 27001:2013 standard, govern all areas of security applicable to the Services, including physical access, system access, data access, transmission, input, security oversight, and enforcement." *See* https://www.oracle.com/legal/privacy/services-privacy-policy/#1-4 (last visited Apr. 9, 2025).

the services it provides; and provide adequate notice to patients if their Private Information is disclosed without authorization.

40. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Oracle assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

41. Without the required submission of Private Information from Plaintiffs and Class Members, Defendant could not perform the services it provides.

42. Plaintiffs and Class Members relied on Oracle to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. <u>The Data Breach and Defendant's Inadequate Notice to Plaintiffs and Class Members</u>

43. As described herein, Defendant detected unauthorized access to its legacy Cerner servers on or around February 20, 2025, with such unauthorized access starting on or after January 22, 2025.

44. At some point after February 20, 2025 Oracle sent notices to impacted customers informing them of a "cybersecurity event involving unauthorized access to some amount of your Cerner data that was on an old legacy server not yet migrated to the Oracle Cloud."[13]

45. Oracle has not sent Data Breach notices to any of the Plaintiffs and Class Members. In fact, it was reported that Oracle is telling hospitals that it will not be notifying patients directly

[13] *See Oracle Health breach compromises patient data at US hospitals, supra* note 4.

and that it is the hospitals' responsibility to determine if the stolen data violates HIPAA laws and whether they are required to send notifications.[14]

46. Oracle has not disclosed the details of the cyberattack with its customers or its customers' patients, including root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

47. This "disclosure" amounts to no real disclosure at all, as it fails to inform Oracle's customers as well as Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

48. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

49. The attacker accessed and acquired files in Defendant's servers containing unencrypted Private Information of Plaintiffs and Class Members, including, upon information and belief, their names, Social Security numbers, and health and/or clinical information.

50. Oracle offered absolutely zero substantive steps to help victims like Plaintiffs and Class Members protect themselves.

---

[14] *See id.*

51. Oracle had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

52. Plaintiffs and Class Members provided their Private Information to Oracle with the reasonable expectation and mutual understanding that Oracle would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

53. Oracle's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

54. Oracle knew or should have known that its electronic records would be targeted by cybercriminals.

C. The Healthcare Sector is Particularly Susceptible to Data Breaches

55. Oracle was on notice that healthcare entities are particularly susceptible targets for data breaches.

56. Oracle was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[15]

[15] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited Apr. 9, 2025).

57. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[16]

58. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[17] In 2022, the largest growth in compromises occurred in the healthcare sector.[18]

59. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020. Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[19] The 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

---

[16] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Apr. 9, 2025).

[17] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, https://www.idtheftcenter.org/2018-data-breaches/ (last visited Apr. 9, 2025).

[18] Identity Theft Resource Center, *2022 End-of-Year Data Breach Report*, https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited Apr. 9, 2025).

[19] *See* Identity Theft Resource Center, *2021 Data Breach Annual Report*, 6 (Jan. 2022), https://notified.idtheftcenter.org/s/ (last accessed Feb. 15, 2024).

60. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

61. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[20]

62. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[21]

[20] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited Apr. 9, 2025).

[21] *Id*.

63. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[22]

64. A ransomware attack is a type of cyberattack that is frequently used to target healthcare providers due to the sensitive patient data they maintain. In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network. Ransomware attacks are particularly harmful for patients and healthcare providers alike as they cause operational disruptions that result in lengthier patient stays, delayed procedures or test results, increased complications from surgery, and even increased mortality rates. In 2021, 44% of healthcare providers who experienced a ransomware attack saw their operations disrupted for up to a week and 25% experienced disrupted services for up to a month.[23]

65. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data

[22] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited Apr. 9, 2025).

[23] Sophos, *The State of Ransomware in Healthcare 2022* (May 2022), https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf

contained within.[24] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[25] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[26] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[27]

66. Accordingly, Plaintiffs and Class Members believe that their Private Information was or will be sold on the dark web, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

67. As a healthcare services vendor, Oracle knew, or should have known, the importance of safeguarding its clients' patients' Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on Oracle's clients' patients as a result of a breach. Oracle failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

D. Oracle Failed to Comply with HIPAA

68. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that the Department of Health

---

[24] *The chance of data being stolen in a ransomware attack is greater than one in ten* (July 13, 2020), https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/

[25] *2020 Quarterly Report: Ransomware Demands continue to rise as Data Exfiltration becomes common and Maze subdues* (November 4, 2020), https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[26] *Id.*

[27] *Id.*

and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

69. Oracle's Data Breach resulted from a combination of insufficiencies that indicate Oracle failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Oracle's Data Breach that Oracle either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiffs' and Class Members' PHI.

70. Plaintiffs' and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

71. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

72. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

73. Plaintiffs' and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

74. Plaintiffs' and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

75. Upon information and belief, Oracle reasonably believes that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

76. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

77. Upon information and belief, Oracle reasonably believes that Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

78. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

79. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

80. It is reasonable for Plaintiffs and Class Members to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

81. Oracle's Data Breach could have been prevented if Oracle had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

82. Oracle's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Oracle creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

83. While monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure Oracle's approach to information security is adequate and appropriate going forward. Oracle still maintains the PHI and other highly sensitive PII of its customers' current and former patients, including Plaintiffs and Class Members. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent data breaches.

E. Oracle Failed to Comply with FTC Guidelines

84. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

85. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

86. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

87. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

88. As evidenced by the Data Breach, Oracle failed to properly implement basic data security practices. Oracle's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

89. Oracle was at all times fully aware of its obligation to protect the Private Information of its customers' patients yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Oracle Failed to Comply with Industry Standards

90. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

91. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like Oracle include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

92. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training

staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

93. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

94. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

G. Oracle Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information

95. In addition to its obligations under federal and state laws, Oracle owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Oracle owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

96. Oracle breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems, servers and data. Oracle's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect its customers' patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its customers' clients' Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

97. Oracle negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

98. Had Oracle remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

99. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with Oracle.

H. Oracle Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft

100. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such

as data breaches or unauthorized disclosure of data.[28] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

101. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

102. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

103. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information

[28] *FTC Information Injury Workshop, BE and BCP Staff Perspective* (October 2018), https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited Apr. 9, 2025).

to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

104. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

105. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[29] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

106. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including medical identity theft, credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information.

[29] *See* FTC, *IdentityTheft.gov*, https://www.identitytheft.gov/Steps (last visited Apr. 9, 2025).

107. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[30]

108. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

109. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[31]

110. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

111. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial

---

[30] FTC, *Warning Signs of Identity Theft*, https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited Apr. 9, 2025).

[31] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited Apr. 9, 2025).

repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[32]

112. The ramifications of Oracle's failure to keep its customers' patients' Private Information secure are long-lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

113. The value of PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

114. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[33]

115. For example, Social Security numbers are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as may be experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use

[32] Michael Ollove, "*The Rise of Medical Identity Theft in Healthcare*," Kaiser Health News (Feb. 7, 2014), https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited Apr. 9, 2025).

[33] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Apr. 9, 2025).

> your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[34]

116. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

117. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[35]

118. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[36]

---

[34] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Apr. 9, 2025).

[35] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Apr. 9, 2025).

[36] GAO,*Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/assets/270/262904.html (last visited Apr. 9, 2025).

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

119. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

120. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

I. Plaintiffs' Experiences and Damages

Plaintiff Rebecca Blount's Experience

121. Plaintiff Blount received medical services and treatment from one of Oracle's client hospital systems that uses Cerner software.

122. As a condition of receiving medical services and treatment from Oracle's client, Plaintiff Blount was required to provide Defendant with substantial amounts of her PII and PHI.

123. Upon information and belief, at the time of the Data Breach Oracle retained Plaintiff Blount's Private Information in its systems.

124. Plaintiff is very careful about sharing her sensitive PII and PHI. She stores any documents containing PII or PHI in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source.

125. Plaintiff Blount greatly values her privacy, and would not have provided her Private Information to Defendant, undertaken the services and paid the amounts she had for medical services had Defendant timely disclosed that its systems lacked adequate computer and data

security practices to safeguard its customers' clients' personal and health information from theft, and that those systems were subject to a data breach.

126. Upon information and belief, Plaintiff Blount suffered actual injury in the form of having her Private Information compromised and/or stolen as a result of the Data Breach, including but not limited to (a) damage to and diminution in the value of her personal, health, and financial information – a form of intangible property that Plaintiffs entrusted to Defendant for the purpose of receiving healthcare services from Defendant and/or Defendant's client; (b) violation of privacy rights; and (c) substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

127. As a result of the Data Breach, Plaintiff Blount anticipates spending considerable time and money on an ongoing basis to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and protecting herself from medical fraud.

128. As a result of the Data Breach, Plaintiff Blount has suffered anxiety as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of committing cyber and other crimes against her including, but not limited to, fraud and identity theft. Plaintiff Blount is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on her life.

129. Plaintiff Blount has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

Plaintiff Cheryl McCulley's Experience

130. Plaintiff McCulley received medical services and treatment from one of Oracle's client hospital systems that uses Cerner software.

131. As a condition of receiving medical services and treatment from Oracle's client, Plaintiff McCulley was required to provide Defendant with substantial amounts of her PII and PHI.

132. Upon information and belief, at the time of the Data Breach Oracle retained Plaintiff McCulley's Private Information in its systems.

133. Plaintiff is very careful about sharing her sensitive PII and PHI. She stores any documents containing PII or PHI in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source.

134. Plaintiff McCulley greatly values her privacy, and would not have provided her Private Information to Defendant, undertaken the services and paid the amounts she had for medical services had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its customers' clients' personal and health information from theft, and that those systems were subject to a data breach.

135. Upon information and belief, Plaintiff McCulley suffered actual injury in the form of having her Private Information compromised and/or stolen as a result of the Data Breach, including but not limited to (a) damage to and diminution in the value of her personal, health, and financial information – a form of intangible property that Plaintiffs entrusted to Defendant for the purpose of receiving healthcare services from Defendant and/or Defendant's client; (b) violation of privacy rights; and (c) substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

136. As a result of the Data Breach, Plaintiff McCulley anticipates spending considerable time and money on an ongoing basis to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and protecting herself from medical fraud.

137. As a result of the Data Breach, Plaintiff McCulley has suffered anxiety as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of committing cyber and other crimes against her including, but not limited to, fraud and identity theft. Plaintiff McCulley is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on her life.

138. Plaintiff McCulley has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

J. Common Injuries and Damages

139. As a direct and proximate result of Oracle's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

140. Further, and as set forth above, as a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members will be forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or

modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

141. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

142. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

143. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

144. Plaintiffs and Class Members also lost the benefit of the bargain they made with Oracle. Plaintiffs and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price paid by Plaintiffs and Class Members (or, in some cases, on their behalf) to Oracle was intended to be used by Oracle to fund adequate security of Oracle's system and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive the benefit of the bargain.

145. Additionally, Plaintiffs and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth

roughly $200 billion.[37] In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker who in turn aggregates the information and provides it to other companies.[38] Consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[39]

146. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

147. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;
b. Canceling and reissuing credit and debit cards;
c. Addressing their inability to withdraw funds linked to compromised accounts;
d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

[37] *See* Data Coup, *The personal data revolution*, https://datacoup.com/ (last visited Apr. 9, 2025).

[38] *What is digi.me?*, https://digi.me/what-is-digime/ (last visited Apr. 9, 2025).

[39] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Apr. 9, 2025).

e. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
f. Contacting financial institutions and closing or modifying financial accounts;
g. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;
h. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and
i. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

148. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Oracle, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of its customers' patients is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

149. As a direct and proximate result of Oracle's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

CLASS ACTION ALLEGATIONS

150. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Rule 23 of the Federal Rule of Civil Procedure, on behalf of the following Nationwide Class, subject to amendment as appropriate:

Nationwide Class

All individuals whose Private Information was compromised in the Data Breach.

151. Plaintiff McCulley brings this action individually and on behalf of the following California Subclass:

California Subclass

All individuals residing in California whose Private Information was compromised in the Data Breach.

152. The Nationwide Class and the California New York Subclass are collectively referred to herein as the "Class."

153. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

154. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

155. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

156. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of Class Members are ascertainable through Oracle's and its customers' records, including but not limited to, the files implicated in the Data Breachs.

157. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Oracle engaged in the conduct alleged herein;

b. When Oracle learned of the Data Breach;

c. Whether Oracle's response to the Data Breach was adequate;

d. Whether Oracle unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

e. Whether Oracle failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether Oracle's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether Oracle's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Oracle owed a duty to Class Members to safeguard their Private Information;

i. Whether Oracle breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether Oracle had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

l. Whether Oracle breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

m. Whether Oracle knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiffs and Class Members suffered as a result of Oracle's misconduct;

o. Whether Oracle's conduct was negligent;

p. Whether Oracle's conduct was *per se* negligent;

q. Whether Oracle was unjustly enriched;

r. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

158. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Oracle. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs individually. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

159. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

160. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that Plaintiffs' and Class Members' Private Information was

stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

161. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Oracle. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

162. Finally, all members of the proposed Class are readily ascertainable. Oracle has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Oracle.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
NEGLIGENCE
(On behalf of Plaintiffs and the Nationwide Class)

163. Plaintiffs restate and reallege all of the allegations in every preceding paragraph as if fully set forth herein.

164. Oracle knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

165. Oracle knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Oracle was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

166. Oracle owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Oracle's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect its customers' clients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to federal and state regulations including but not limited to HIPAA and the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

167. Oracle's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

168. Oracle's duty also arose because as a service provider Defendant was bound by industry standards to protect its customers' clients' confidential Private Information.

169. Oracle holds itself out as a trusted data collector, and thereby assumes a duty to reasonably protect its customers' clients' information. Indeed, Defendant, as a direct data collector, was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

170. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Oracle owed them a duty of care to not subject them to an unreasonable risk of harm.

171. Oracle, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Oracle's possession.

172. Oracle, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

173. Oracle, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

174. Oracle breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA; and

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised.

175. Oracle had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Oracle and its customers with their Private Information was predicated on the understanding that Oracle would take adequate security precautions. Moreover, only Oracle had the ability to protect its systems (and the Private Information that it stored on them) from attack.

176. Oracle's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised, exfiltrated, and/or misused, as alleged herein.

177. As a result of Oracle's ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

178. Oracle's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

179. As a result of Oracle's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

180. As a direct and proximate result of Oracle's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

181. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

182. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

183. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Oracle to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

SECOND CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of Plaintiffs and the Nationwide Class)

184. Plaintiffs restate and reallege the allegations in every preceding paragraph as if fully set forth herein.

185. Upon information and belief, Defendant entered into virtually identical and valid contracts with its customers to provide software products and/or services, including business associate agreements under HIPAA, which included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be entrusted to it.

186. Such contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their Private Information that Defendant agreed to receive and protect through its services.

187. The benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties, and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

188. Plaintiffs and the Class are also intended third-party beneficiaries of these contracts because recognizing them as such is appropriate to effectuate the intentions of the parties, and the circumstances indicate that Defendant intended to give the beneficiaries the benefit of the promised performance.

189. Defendant knew that if they were to breach these contracts, healthcare patients including Plaintiffs and the Class, would be harmed by, among other harms, fraudulent transactions.

190. Defendant breached its contracts when it failed to use reasonable data security measures and/or business associate monitoring measures, and allowed the Data Breach to occur.

191. As foreseen, Plaintiffs and the Class were harmed by Defendant's failure to use reasonable data security measures to securely store and protect the files in its care, including but not limited to, the continuous and substantial risk of harm through the loss of their Private Information. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Nationwide Class)

192. Plaintiffs restate and reallege the allegations in every preceding paragraph as if fully set forth herein.

193. Plaintiffs bring this claim in the alternative to their breach of third-party beneficiary contract cause of action.

194. Oracle provides healthcare-related services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for services from Defendant (or having their insurance companies pay Defendant on their behalf).

195. Through Defendant's sale of medical services, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with Oracle's policies, practices, and applicable law.

196. As consideration, Plaintiffs and Class Members paid money (or money was paid on their behalf) to Oracle and turned over valuable Private Information to Oracle. Accordingly, Plaintiffs and Class Members bargained with Oracle to securely maintain and store their Private Information.

197. Defendant solicited, offered and invited Plaintiffs and Class members to provide their Private Information as part of Oracle's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Oracle or to doctors or other healthcare professionals who then provided it to Defendant.

198. Oracle accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing healthcare-related services to Plaintiffs and Class Members.

199. In delivering their Private Information to Oracle and paying for healthcare services, Plaintiffs and Class Members intended and understood that Oracle would adequately safeguard the Private Information as part of that service.

200. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA standards to make sure that Plaintiffs' and Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

201. Plaintiffs and Class Members would not have entrusted their Private Information to Oracle in the absence of such an implied contract.

202. Had Oracle disclosed to Plaintiffs and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to Oracle.

203. As a provider of healthcare-related services, Oracle recognized (or should have recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must

be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the other Class Members.

204. Oracle violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information. Oracle further breached these implied contracts by failing to comply with its promise to abide by HIPAA.

205. Additionally, Oracle breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

206. Oracle also breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

207. Oracle further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

208. Oracle further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

209. Oracle further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

210. Oracle further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

211. Oracle further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations, in violation of 45 CFR 164.306(a)(94).

212. Oracle further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq*.

213. Oracle further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

214. Oracle further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

215. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide accurate and complete Private Information and to pay Oracle in exchange for Oracle's agreement to, *inter alia*, protect their Private Information.

216. Plaintiffs and Class Members have been damaged by Oracle's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class)

217. Plaintiffs restate and reallege the allegations in every preceding paragraph as if fully set forth herein.

218. This cause of action is pleaded in the alternative to Plaintiffs' second and third causes of action above.

219. Plaintiffs and Class Members conferred a benefit on Oracle by turning over their Private Information to Defendant and by paying for medical services (or having their insurance companies pay for medical services) that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

220. Upon information and belief, Oracle funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiffs and Class Members (or on their behalf).

221. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Oracle.

222. Oracle has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

223. Oracle knew that Plaintiffs and Class Members conferred a benefit upon it, which Oracle accepted. Oracle profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

224. If Plaintiffs and Class Members had known that Oracle had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

225. Due to Oracle's conduct alleged herein, it would be unjust and inequitable under the circumstances for Oracle to be permitted to retain the benefit of its wrongful conduct.

226. As a direct and proximate result of Oracle's conduct, Plaintiffs and Class Members have suffered and/ or are at a continual substantial and imminent risk of suffering, injury, including but not limited to: (i) identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Oracle's possession and is subject to further unauthorized disclosures so long as Oracle fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

227. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Oracle and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Oracle from its wrongful conduct. This can be accomplished by

establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

228. Plaintiffs and Class Members may not have an adequate remedy at law against Oracle, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

FIFTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(On behalf of Plaintiffs and the Nationwide Class)

229. Plaintiffs restate and reallege the allegations in every preceding paragraph as if fully set forth herein.

230. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Oracle and ultimately accessed and acquired in the Data Breach.

231. As a healthcare service provider, Oracle has a special relationship with its customers' patients, including Plaintiffs and Class Members. Because of that special relationship, Oracle was provided with and stored Plaintiffs' and Class Members' Private Information and had a duty to maintain such Information in confidence.

232. Patients like Plaintiffs and Class Members have a privacy interest in personal medical and other matters, and Oracle had a duty not to disclose such matters concerning its customers' patients.

233. As a result of the parties' relationship, Oracle had possession and knowledge of highly sensitive and confidential PHI and PII belonging to Plaintiffs and Class Members, information that was not generally known.

234. Plaintiffs and Class Members did not consent nor authorize Defendant to release or disclose their Private Information to an unknown criminal actor.

235. Oracle breached its duty of confidence owed to Plaintiffs and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of Plaintiffs' and Class Members' Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement adequate information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers' patients; and (h) making an unauthorized and unjustified disclosure and release of Plaintiffs' and Class Members' Private Information to a criminal third party.

236. But for Oracle's wrongful breach of its duty of confidence owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

237. As a direct and proximate result of Oracle's wrongful breach of its duty of confidence, Plaintiffs and Class Members have suffered and will continue to suffer the injuries alleged herein.

238. It would be inequitable for Oracle to retain the benefit of controlling and maintaining Plaintiffs' and Class Members' Private Information at the expense of Plaintiffs and Class Members.

239. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

SIXTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs and the Nationwide Class)

240. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

241. In providing their Private Information to Defendant, Plaintiffs and Class Members justifiably placed a special confidence in Defendant to act in good faith and with due regard for the interests of Plaintiffs and Class Members to safeguard and keep confidential that Private Information.

242. As a healthcare service provider, Defendant has a fiduciary relationship to its customers and their clients, like Plaintiffs and Class Members.

243. Because of that fiduciary relationship, Oracle was provided with and stored valuable and sensitive Private Information belonging to Plaintiffs and Class Members, which it was required to maintain in confidence.

244. Defendant accepted the special confidence its customers, Plaintiffs and Class Members placed in it.

245. In light of the special relationship between Defendant, Plaintiffs, and Class Members, whereby Defendant became a guardian of Plaintiffs and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiffs and Class Members for the safeguarding of Plaintiffs and Class Members' Private Information.

246. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its customer relationships, in particular, to keep secure the Private Information of its customers' patients, exercise utmost care in protecting the Private Information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons, and to timely notify Plaintiffs and Class Members of a data breach and disclosure.

247. Plaintiffs and Class Members have a privacy interest in their Private Information.

248. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

249. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs and Class Members' Private Information and by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

250. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to:

a. The compromise, publication, and/or theft of their Private Information;

b. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;

c. Lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft;

d. The continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession;

e. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members and

f. The diminished value of the services they paid for and received.

251. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members will suffer other forms of injury and/or harm, and other economic and non-economic losses.

SEVENTH CAUSE OF ACTION
BAILMENT
(On behalf of Plaintiffs and the Class)

252. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

253. Defendant acquired and was obligated to safeguard the Private Information of Plaintiffs and Class Members.

254. Defendant accepted possession and took control of Plaintiffs' and Class Members' Private Information under such circumstances that the law imposes an obligation to safeguard the property of another.

255. Specifically, a constructive bailment arises when Defendant, as is the case here, takes lawful possession of the property of another and has a duty to account for that property, without intending to appropriate it.

256. Constructive bailments do not require an express assumption of duties and may arise from the bare fact of the thing coming into the actual possession and control of a person fortuitously, or by mistake as to the duty or ability of the recipient to affect the purpose contemplated by the absolute owner.

257. During the bailment, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care, diligence and prudence in protecting their Private Information.

258. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class Members' Private Information, resulting in the unlawful and unauthorized access to and misuse of such Information.

259. Defendant further breached its duty to safeguard Plaintiffs' and Class Members' Private Information by failing to notify them individually in a timely and accurate manner that their Private Information had been breached and compromised.

260. As a direct and proximate result of Defendant's breach of duty, Plaintiffs and Class Members have suffered compensable damages that were reasonably foreseeable to Defendant, including but not limited to, the damages set forth herein.

EIGHTH CAUSE OF ACTION
INVASION OF PRIVACY
(On behalf of Plaintiffs and the Nationwide Subclass)

261. Plaintiffs restate and reallege the allegations in every preceding paragraph as if fully set forth herein.

262. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

263. As a result of Defendant's conduct, publicity was given to Plaintiffs' and Class Members' Private Information, which necessarily includes matters concerning their private life such as PII and PHI.

264. A reasonable person of ordinary sensibilities would consider the publication of Plaintiffs' and Class Members' Private Information to be highly offensive.

265. Plaintiffs' and Class Members' Private Information is not of legitimate public concern and should remain private.

266. As a direct and proximate result of Defendant's public disclosure of private facts, Plaintiffs and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

267. Plaintiffs and Class Members are entitled to compensatory, consequential and nominal damages suffered as a result of the Data Breach.

268. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, (i) strengthen its data security systems and monitoring procedures;

(ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

NINTH CAUSE OF ACTION
VIOLATIONS OF THE CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code §§ 1798.80 *et seq*.
(On behalf of Plaintiff McCulley and the California Subclass)

269. Plaintiff McCulley restates and realleges the allegations in every preceding paragraph as if fully set forth herein.

270. Plaintiff brings this claim individually and on behalf of the California Subclass Class (the "Class" for purposes of this count).

271. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

272. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

273. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

274. Plaintiff and the Class Members are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Defendant for the purpose of obtaining a product and/or service from Defendant.

275. The personal information of Plaintiff and the Class Members at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

276. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Plaintiff's and Class Members' personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the Class Members. Specifically, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiff and the Class Members from unauthorized access, destruction, use, modification, or disclosure. Defendant further subjected Plaintiff's and the Class Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's

violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

277. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiff and the Class Members included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and the Class Members by the cyber attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

278. As a direct and proximate result of Defendant's acts or omissions, Plaintiff and the Class Members were injured and lost money or property including, but not limited to, the loss of Plaintiff's and the Class Members' legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

279. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

280. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;
b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

   i. the date of the breach,

   ii. the estimated date of the breach, or

   iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

281. Defendant failed to provide the legally compliant notice under § 1798.82(d) to Plaintiff and members of the Class. On information and belief, to date, Defendant has not sent written notice of the data breach to all impacted individuals. As a result, Defendant has violated § 1798.82 by not providing legally compliant and timely notice to all Class Members. Because not all members of the class have been notified of the breach, members could have taken action to

protect their personal information, but were unable to do so because they were not timely notified of the breach.

282. On information and belief, many Class Members affected by the breach have not received any notice at all from Defendant in violation of Section 1798.82(d).

283. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and Class Members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

284. As a direct consequence of the actions as identified above, Plaintiff and Class Members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

TENTH CAUSE OF ACTION
VIOLATIONS OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT
Cal. Civ. Code §§ 56 *et seq*.
(On behalf of Plaintiff McCulley and the California Subclass)

285. Plaintiff McCulley restates and realleges the allegations in every preceding paragraph as if fully set forth herein.

286. Plaintiff brings this claim individually and on behalf of the California Subclass Class (the "Class" for purposes of this count).

287. Under the California Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq*. (hereinafter referred to as the "CMIA"), "medical information" means "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment." Cal. Civ. Code § 56.05.

288. Additionally, Cal. Civ. Code § 56.05 defines "individually identifiable" as meaning that "the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual." Cal. Civ. Code § 56.05.

289. Under Cal. Civ. Code § 56.101(a) of the CMIA,

> (a) Every provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein.
>
> Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36.

Cal. Civ. Code § 56.101.

290. At all relevant times, Defendant was a health care contractor within the meaning of Civil Code § 56.05(d) because it is a "medical group, independent practice association, pharmaceutical benefits manager, or medical service organization and is not a health care service plan or provider of health care." In the alternative, Defendant is a health care provider within the

meaning of Civil Code § 56.06(b) because it maintains medical information as defined by Civil Code § 56.05.

291. Plaintiff and Class Members are Defendant's patients, as defined in Civil Code § 56.05(k).

292. Plaintiff and Class Members provided their personal medical information to Defendant.

293. At all relevant times, Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of medical information in the ordinary course business.

294. As a result of the Data Breach, Defendant has misused, disclosed, and/or allowed third parties to access and view Plaintiff's and Class Members' personal medical information without their written authorization compliant with the provisions of Civil Code §§ 56, *et seq*. As a further result of the Data Breach, the confidential nature of the Plaintiff's medical information was breached as a result of Defendant's negligence. Specifically, Defendant knowingly allowed and affirmatively acted in a manner that actually allowed unauthorized parties to access and view Plaintiff's and Class Members' Private Information, which was viewed and used when the unauthorized parties engaged in the above-described fraudulent activity. Defendant's misuse and/or disclosure of medical information regarding Plaintiff and Class Members constitutes a violation of Civil Code §§ 56.10, 56.11, 56.13, and 56.26.

295. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care, Plaintiff's and Class Members' personal medical information was disclosed without written authorization.

296. By disclosing Plaintiff's and Class Members' Private Information without their written authorization, Defendant violated California Civil Code § 56, et seq., and its legal duty to protect the confidentiality of such information.

297. Defendant also violated Sections 56.06 and 56.101 of the California CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

298. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff's and Class Members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiff's and Class Members' written authorization.

299. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violation of the CMIA, Plaintiff and Class Members are entitled to (i) actual damages, (ii) nominal damages of $1,000 per Plaintiff and Class Member, (iii) punitive damages of up to $3,000 per Plaintiff and Class Member, and (iv) attorneys' fees, litigation expenses and court costs under California Civil Code § 56.35.

ELEVENTH CAUSE OF ACTION
VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code §§ 17000 *et seq*.
(On behalf of Plaintiff McCulley and the California Subclass)

300. Plaintiff McCulley restates and realleges the allegations in every preceding paragraph as if fully set forth herein.

301. Plaintiff brings this claim individually and on behalf of the California Subclass Class (the "Class" for purposes of this count).

302. Defendant is a "person" defined by Cal. Bus. & Prof. Code § 17201.

303. Defendant violated Cal. Bus. & Prof. Code § 17200 *et seq*. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

304. Defendant's "unfair" acts and practices include:

a. Defendant failed to implement and maintain reasonable security measures to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 *et seq*.), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. Defendant's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

305. Defendant has engaged in "unlawful" business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45, and California common law.

306. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' personal information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' personal information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' personal information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

307. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' personal information.

308. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class Members were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

309. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

310. Plaintiff and Class Members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

311. By deceptively storing, collecting, and disclosing their personal information, Defendant has taken money or property from Plaintiff and Class Members.

312. By deceptively storing, collecting, and disclosing their personal information, Plaintiff and Class Members overpaid Defendant for services that did not include proper data security for their Private Information.

313. Plaintiff and Class Members would not have provided their Private Information to Defendant or paid Defendant money for services if Plaintiff and Class Members had known that Defendant's data security measures were inadequate to protect their Private Information.

314. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and Class Members' rights.

315. Plaintiff and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

TWELTH CAUSE OF ACTION
VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code § 1798.150
(On behalf of Plaintiff McCulley and the California Subclass)

316. Plaintiff McCulley restates and realleges the allegations in every preceding paragraph as if fully set forth herein.

317. Plaintiff brings this claim individually and on behalf of the California Subclass Class (the "Class" for purposes of this count).

318. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of

the information to protect the nonencrypted PII/PHI of Plaintiff and the California Subclass. As a direct and proximate result, Plaintiff's and the California Subclass's nonencrypted and nonredacted PII/PHI was subject to unauthorized access and exfiltration, theft, or disclosure.

319. Defendant is a "business" under the meaning of Civil Code § 1798.140.

320. Plaintiff and California Subclass Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards PII/PHI by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold PII/PHI, including Plaintiff's and California Subclass members' PII/PHI. Plaintiff and California Subclass members have an interest in ensuring that their PII/PHI is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

321. Pursuant to California Civil Code § 1798.150(b), Plaintiff mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

322. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

323. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes described above, request judgment against Oracle and that the Court enter an order:

a. Certifying this action as a Class action, defining the Classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper and adequate representatives of the Classes requested herein;

b. Awarding Plaintiffs and Class Members appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. Awarding injunctive and other equitable relief as necessary to protect the interests of the Classes as requested herein;

d. Instructing Oracle to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. Requiring Oracle to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. Requiring Oracle to implement enhanced data security measures in order to better protect the PII and PHI in its possession and control;

g. Awarding Plaintiffs and Class Members prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

h. Awarding such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATE: April 28, 2025

Respectfully submitted,

PEIFFER WOLF CARR
KANE CONWAY & WISE, LLP

By: */s/ Brandon M. Wise*
Brandon M. Wise - MO Bar # 67242
One US Bank Plaza, Suite 1950
St. Louis, MO 63101
Ph: (314) 833-4825
bwise@peifferwolf.com

ALMEIDA LAW GROUP LLC

David S. Almeida*
849 W. Webster Avenue
Chicago, Illinois 60614
Ph: (708) 437-6476
david@almeidalawgroup.com

**pro hac vice* to be sought

Counsel for Plaintiffs & the Proposed Class